X

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants Counterclaim-Plaintiffs.	Civil Action No. 04-CV-1199 (SLR)

DECLARATION OF FREDERICK AVOLIO

TABLE OF CONTENTS

I, Frederick Michael Avolio, declare that:

1. I am the president and founder of Avolio Consulting, Inc., a Maryland-based corporation specializing in computer and network security.

2. I have been retained by counsel for Symantec Corporation as an expert witness in this action. If called to testify as to the truth of the matters stated herein, I could and would do so competently.

3. I received a Bachelor of Science degree in Computer Science from the University of Dayton in 1977, and a Masters of Science degree in Computer Science from Indiana University in 1979.

4. I worked at Digital Equipment Corporation (DEC) from April 1984-November 1992. While at DEC, I was development manager for the first commercial firewall, the DEC SEAL. I helped design the DEC SEAL and marketed it. DEC SEAL was first installed at DuPont in Wilmington, DE, in June 1991.

5. I worked at Trusted Information Systems, Inc. (TIS) from November 1992-May 1998. While at TIS, I was project leader, then development manager and product manager for both the TIS Firewall Toolkit and the TIS Gauntlet Internet Firewall. In this role in the early 1990s, I was responsible for helping with the architecture of these firewalls and management of the project, which originally was a DARPA contract for the Executive Office of the President. I supervised all aspects of the Firewall Toolkit development, interacted with the customer (DARPA and EOP), and managed the budget. I was also development manager and then product manager for the Gauntlet Internet Firewall, a commercial product, in the mid-90s.

6. I have written about and taught classes on the subject of Internet firewalls since the early 1990s for Networld+Interop (in the US and in France), the Computer Security Institute (in the US, Canada, and Costa Rica), the MIS Training Institute, the SANS Institute, and at the Dnepropetrovsk National University in Ukraine. In the 1990s and 2000s I have

written on the subject of Internet Firewalls for *Information Security Magazine,*[1] *The IP Journal,*[2] the Association for Computing Machinery (ACM) *netWorker* magazine,[3] *Performance Computing,*[4] The Internet Security Conference,[5] USENIX,[6] at the Internet Society's Network and Distributed System Security Symposium,[7] and in various other whitepapers and editorials.[8]

7. A summary of my professional experience and publications are attached as Exhibit A.

8. I receive compensation in the amount of $300.00 per hour for the time that I devote to this matter. My compensation is not dependent in any way on the outcome of this matter.

I. METHODOLOGY AND BASES

9. In preparing my opinions and analysis of the art, I have thoroughly reviewed the entire specification and claims of U.S. Patents No. 6,321,338 (the '338 patent); 6,484,203 (the '203 patent); 6,708,212 (the '212 patent); and 6,711,615 (the '615 patent) (collectively, the patents-in-suit). I have also reviewed each of the prosecution histories associated with the patents-in-suit.

10. I understand that the Court has not yet construed certain claim terms in the claims of the patents-in-suit. Since the Court has not yet issued a decision construing the claims of the patents-in-suit, I have been asked, for purposes of this analysis, to assume that the Court adopts the claim construction positions advanced by SRI.

---

[1] http://www.infosecuritymag.com/2003/apr/testcenter.shtml; http://www.infosecuritymag.com/2003/feb/gatewayguardians.shtml; http://infosecuritymag.techtarget.com/articles/1999/maycover.shtml.
[2] http://www.avolio.com/papers/fw2hundred.html.
[3] http://www.avolio.com/articles/MultiDimensional.html.
[4] http://www.avolio.com/articles/UR_castle-def.html.
[5] http://www.avolio.com/papers/rise+fall.html.
[6] http://www.avolio.com/papers/fwtk.html.
[7] http://www.avolio.com/papers/isoc.html.
[8] http://www.avolio.com/sec.html; http://www.avolio.com/articles/fw+vpns.html; http://www.avolio.com/papers/sectyoninet.html.

11. I have reviewed an extensive body of prior art publications. A list of the prior art publications and documentation I have reviewed and the individuals with whom I have spoken in forming the opinions set forth below is attached as Exhibit B.

12. In particular, I reviewed in detail the publication *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, by P. Porras and P. Neumann, 20th National Information Systems Security Conference, October 7, 1997 (hereinafter, *Emerald 1997*).

II. SUMMARY OF OPINIONS

13. The *Emerald 1997* publication discloses that logs from entities such as firewalls may be used to gather event data for analysis. In light of this disclosure, one of skill in the art would have understood from this publication that certain categories of network traffic data should be monitored and analyzed. Firewalls in 1997 monitored and logged: (1) network connections, including both network connection requests and denials, (2) data transfers, including network packet data volume and network packet data transfer volume. Thus, monitoring all of these network traffic data categories is disclosed in the *Emerald 1997* publication.

14. Furthermore, because *Emerald 1997* disclosed deploying monitors at network infrastructure such as a firewall, it also disclosed deploying a monitor at a proxy server.

III. INTRODUCTION

A. A BRIEF HISTORY OF COMPUTER SECURITY TECHNIQUES

15. Computer security techniques are used to preserve and protect the volumes of data and applications that reside on different computer systems. As computers and computer networks have become larger and more valuable, the need to protect them has grown as well. Intrusion detection systems ("IDS") are an outgrowth of the need for computer security, because they are designed to detect, and in some cases thwart, unwanted attempts to infiltrate or access a computer. An "intrusion" can refer to any type of anomalous, illicit, or prohibited

activity. An intrusion may originate from an external threat, or misuse by an internal user. Intrusion detection systems have been described as "a burglar alarm for computers and networks."[9]

16. It is difficult to pinpoint a beginning in the development of intrusion detection systems, because interest in protecting computer systems has been a natural consequence of the growth of the computer industry. Intrusion detection systems have progressed from centralized, multi-user systems relying upon audit-based analysis sources to network-based systems utilizing network packet analysis sources. The transition from using mainly "host-based" audit trail analysis (sources internal to individual computers), to the addition of the use of network-centric analysis, requires explanation in order to put the alleged inventions of the patents-in-suit into context.

17. The U.S. Department of Defense ("DOD") funded an extensive "trusted systems" initiative in the 1970's to provide computer system security for the processing of classified information. [10] As part of this program, the DOD created a policy for implementing certain auditing functions for computer networks to track ongoing behavior and provide a mechanism for discovering potential problems.[11] An audit trail is commonly thought of as a paper trail used to track and verify accounting entries. However, in computing, the term refers to a mechanism for recording activities for later examination and verification. An audit trail may track basic operating system functions, such as system calls and processes performed, or it may track application usage or data access.[12] An "audit trail" may also be called an "audit log."

---

[9] R. Bace, INTRUSION DETECTION (Macmillan Technical Publishing 2000).
[10] The U.S. Government has played an important role in the development of IDS through various security initiatives. The patents-in-suit state that they were supported by Government funding from DARPA.
[11] *See* R. Bace, INTRUSION DETECTION at 11 (discussing the DOD's "Tan Book" entitled "A Guide to Understanding Audit in Trusted Systems").
[12] *See* S. Garfinkel and G. Spafford, PRACTICAL UNIX & INTERNET SECURITY at 289-92 (O'Reilly and Assoc. 2nd ed. 1996).

18. Many early intrusion detection systems focused upon the analysis of audit trail information. Such analysis is sometimes referred to as "host-based" because it relies upon information generated on a particular "host" or computer. However, with the proliferation of large computer networks and the likelihood of network-based attacks increasing, intrusion detection systems began focusing upon network traffic and network sources for attack. For example, in the early 1990's, the Network System Monitor ("NSM") developed at the University of California at Davis targeted computer networks and analyzed packet data.[13]

19. As the inventors of the patents-in-suit have acknowledged, the use of packet data in the context of network monitoring is quite old, and has been studied extensively in both the IDS field and many other areas of computing.[14] Packet-switched networks were first developed by the DOD for the Advanced Research Projects Agency Network ("ARPANET") in the late 1960s, which eventually became the Internet we know today.[15] "A packet-switching network handles information in small units, breaking long messages into multiple packets before routing."[16] In the 1970-80s, early Internet researchers began developing a standard communication protocol for the Internet. This protocol suite became known as TCP/IP

---

[13] See R. Bace, INTRUSION DETECTION at 18-19; L.T. Heberlein et al., *A Method to Detect Intrusive Activity in a Networked Environment*, Proceedings of the Fourteenth National Computer Security Conference, at 362-71, Washington, D.C., 1-4 Oct. 1991, NIST/NCSC.

[14] The inventors have stated that the concepts of network monitoring and the use of packet monitoring in IDS are not new. *See* P. Porras and A. Valdes, *Live Traffic Analysis of TCP/IP Gateways*, Nov. 10, 1997 at p. 3 (noting that "[n]etwork monitoring, in the context of fault detection and diagnosis for computer network and telecommunication environments, has been studied extensively by the network management and alarm correlation community" and "[b]oth [the NSM and NADIR systems] performed broadcast LAN packet monitoring to analyze traffic patterns for known hostile or anomalous activity.").

[15] *See* http://www.isoc.org/internet/history/brief.shtml. Note that the Internet should not be confused with the World Wide Web ("WWW"). The Internet is the worldwide collection of TCP/IP networks and gateways, whereas the WWW is the worldwide set of interlinked hypertext documents residing on HTTP ("hyper text transfer protocol") servers. *See* definitions of "Internet" and "World Wide Web" in COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997).

[16] *See* definition of "packet switching" in COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997).

("Transmission Control Protocol/Internet Protocol").[17] TCP/IP can provide a common format for packet-level analysis by various types of intrusion detection systems and other security-related network infrastructure.[18]

20. In conjunction with the growth of networks generally and the Internet in particular, a wide variety of different types of computer equipment were developed to handle the routing and monitoring of network traffic and network packets. For example, routers and gateways were required early in the development of the Internet to connect the various proliferating networks.[19] Routers and gateways receive packets and forward them to their correct destinations based upon the address in each packet's header.

B. THE DEVELOPMENT OF FIREWALLS

21. A key system used by many, if not most, organizations today to protect their private networks is a firewall. A firewall is a set of software programs designed to run on either specialized hardware or on a standard computer box. A firewall is often installed on a specially designated computer so that it remains separate from the rest of the private network and no incoming network request can access private network resources directly. Larger organizations may include several firewalls to isolate particular security domains, where all the machines in the security domain are under the same administrative control and security policy.

22. A firewall protects the resources of an internal private network from many types of external activity, both accidental and deliberate, that may cause harm to that internal network. For example, a firewall may prevent outsiders from accessing the internal network's data sources. A firewall may also control the external resources that internal users may access. Basically, a firewall examines packets flowing across the boundary it is protecting and determines whether or not a packet should be allowed to be forwarded to its intended destination. The firewall makes this determination on the basis of the security policy set by the

---

[17] *See* http://www.isoc.org/internet/history/brief.shtml.
[18] *See* D. Comer and D. Stevens, INTERNETWORKING WITH TCP/IP, VOL. III, Chap. 18 "Application Level Gateways," (Prentice-Hall 1993).
[19] *See* http://www.isoc.org/internet/history/brief.shtml.

firewall administrator. Standard firewall features include logging and reporting on network traffic seen by the firewall, automatic alarms if certain attack patterns are recognized, and a graphical user interface to configure and manage the firewall.

23. Firewalls in some form have existed since the 1980s.[20] In the 1980s, "packet filters" were developed to assist in monitoring traffic over a network.[21] A packet filter is the simplest type of firewall.[22] Packet filters allow unmodified TCP/IP sessions to cross the firewall, subject to the ruleset and policy enforcement in the firewall. Packet filters typically drop packets based upon an identification of source and destination addresses or ports that the filter ruleset forbids. More complex filters may also be set to filter on additional information, such as the type of protocol or service being used. The packet filter firewall does not rewrite addresses or any other packet header information. More sophisticated packet filters can employ stateful inspection. Stateful packet inspection adds slightly more intelligence and flexibility to packet filters by maintaining session state information for the duration of a session. A session refers to a series of interactions during the span of a single connection between two nodes.

24. The first systems actually referred to as firewalls were developed early in the 1990's to provide a mechanism to block unwanted packets.[23] Other examples of firewalls include application gateways (also called proxy systems/servers) and hybrids.[24] An application proxy or proxy server functions in the following manner: in a firewall using application proxies, the TCP/IP connection is made to the appropriate proxy on one interface of the

---

[20] *See* definition of "firewall" in COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997).
[21] *See* S. McCanne and V. Jacobson, *The BSD Packet Filter: A New Architecture for User-level Packet Capture*, Dec. 19, 1992 (discussing early packet filters such as the 1980 CMU/Stanford Packet Filter).
[22] *See* D. B. Chapman and E. Zwicky, BUILDING INTERNET FIREWALLS Chap. 6 (O'Reilly & Assoc., 1995).
[23] *See* W. Cheswick and S. Bellovin, FIREWALLS AND INTERNET SECURITY – REPELLING THE WILY HACKER (Addison-Wesley Pub. Co. 1994).
[24] *See* W. Cheswick and S. Bellovin, FIREWALLS AND INTERNET SECURITY – REPELLING THE WILY HACKER Chaps. 3-4; D. B. Chapman and E. Zwicky, BUILDING INTERNET FIREWALLS Chaps. 4-7.

firewall. The proxy then rewrites portions of the packet headers and sends them out on a new connection on a different network interface. The second connection is from the proxy to the target. By acting as an intermediary, the proxy separates the internal network from the external network to protect it from outside intrusion. Hybrids combine features of different types of firewalls.

25. Firewalls and the information they generate serve as important data sources for intrusion detection systems.[25] Firewall audit logs record data particular to a firewall type of computer system. Because firewalls monitor network packets flowing through a system, their audit logs necessarily audit network packets. These firewall logs are and were used as aids in debugging problems, information sources for forensic analysis (after an attack), and as input to other system "watchers" looking for problems or changes on a system.

26. According to NIST publication itl97-03,[26] an audit log, or audit trail:

> "maintains a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. ... An audit trail is a series of records of computer events, about an operating system, an application, or user activities. A computer system may have several audit trails, each devoted to a particular type of activity. Audit trails may be used as either a support for regular system operations or a kind of insurance policy or as both of these."

27. As used in computing in general, and computer security in particular, the terms "audit log" and "firewall log" mean similar things. As the NIST publication states, "a computer system may have several audit trails, each devoted to a particular type of activity." A firewall is a type of computer system, and a firewall log is a particular instance of an audit log, or audit trail. However, in traditional audit trails used in early intrusion detection systems, the

---

[25] "Many firewalls, I&A systems, access control systems, and other security devices and subsystems generate their own activity logs. These logs contain information that is, by definition, of security significance; they are therefore of particular value to the intrusion detection process. Including these logs as information sources is an obvious way to improve the quality of the intrusion detection process." R. Bace, INTRUSION DETECTION at 74. The patents-in-suit, as well as *Emerald 1997* all mention the use of firewalls. '338 col. 3:44-45, col. 5:4-414; *Emerald 1997* at 354.

[26] http://csrc.nist.gov/publications/nistbul/itl97-03.txt.

information contained in the log was "host-based" and detailed activities from the viewpoint of a central computer. By contrast, a firewall is designed to monitor activity across a network. Thus, a firewall log necessarily contains information about network traffic flow and the network packets sent through the network the firewall is monitoring. So while the format of audit logs and firewall logs is very similar, the information contained in each may be very different.

C. FIREWALL CAPABILITIES CIRCA 1997

28. The firewall market really began to flower between 1996 and 1997. There were dozens of different companies offering firewall products, many of which have long since vanished. In 1997, Internet connectivity was not universal, and for companies with Internet connections, usually only a fraction of employees had access to services other than electronic mail. Nevertheless, most companies realized the importance of securing the vital and proliferating information stored and exchanged on their computer networks. In order to protect this information, it was desirable to have a mechanism for screening incoming and outgoing communications. Firewalls served this vital purpose, and thus had become quite well-known and popular by 1996.

1. Platforms

29. In 1997, nearly all commercial firewall ran on standard Intel or proprietary RISC-based (Sun, HP, or IBM) computer server platforms. (The Lucent "Brick", which ran a proprietary operating system, Inferno, on a proprietary hardware platform, appeared in approximately December 1997 – January 1998). Most ran modified versions of commercially available operating systems, usually a flavor of Unix. Firewalls running on Windows NT platforms were just becoming available at this point in time, and were often not as feature-rich or stable as the older Unix-based products. The hardware platforms generally supported a minimum of two network interfaces (required by definition for firewall functionality), with some products providing three or more. All products claimed to support 10 Mbs Ethernet

speeds; a very small number claimed to support 100 Mbs Fast Ethernet. Some platforms could be upgraded with hardware-based encryption, which also improved performance.

2. Functionality

30. The purpose of a firewall is to allow selected services to pass between two networks of different security levels, and to deny all other traffic. In 1997, firewalls generally accomplished this using packet filtering, stateful inspection, application-layer proxies or gateways, or some combination of all three. The services supported by most firewalls included:

- Terminal Services (TELNET, Rlogin)
- File Transfer (FTP)
- Electronic Mail (SMTP, POP3)
- World Wide Web (HTTP, SHTTP, SSL)
- Gopher/WAIS
- X Windowing System (X11)
- RealAudio
- USENET News (NNTP)

Generally, application proxy firewalls could also "hide" information by rewriting mail headers, while packet filters did not.

31. Most firewalls included additional functionality, such as:

- Network Address Translation (NAT)
- Virtual Private Network (most vendors offered point to point encrypted tunnels, some using IPSec, but generally not end user VPN capability, which was offered by only two vendors)
- Token-based Authentication (using SecureID, CryptoCard, or similar products)
- Split Domain Name System (DNS)

- A generic proxy or gateway

32. In 1997, content filtering became a hot topic. Some firewalls could be enhanced with third-party virus-checking modules, and could filter HTTP transactions for ActiveX or Java content.

3. Management

33. Ease and simplicity of management was one of the main areas of competition for firewall marketshare in 1997. The early Unix firewalls had text-based interfaces that required operating system expertise, and could be difficult to decipher. The advantage was that they could be flexible and powerful in the hands of an expert; the disadvantage was that many companies just getting onto the Internet didn't have that expertise in house. Some firewalls in 1997 had adopted browser-based interfaces, whereas others used simpler window-based GUIs. Checkpoint's Firewall-1 provided a fairly sophisticated user interface that allowed management of multiple firewalls from a single management point.

34. Firewall products also varied in the flexibility and granularity of configuration options. While market leaders such as Firewall-1, Gauntlet, and Raptor allowed flexible application of rulesets and definition of user groups, other products were more limited.

4. Logging and reporting

35. All of the major firewall products provided some level of logging and event notification, with some variation in the capabilities and features available. Nearly all products logged information about a particular "session" or connection between two points on the network, including: the timestamp of the session, its duration (how long the two point were communicating), the source and destination addresses and ports, and the number of bytes exchanged, as well as any failed or denied attempts to access services. Most products provided at least a minimal level of reporting capability, which usually included options for the firewall administrator to write his or her own scripts for reporting usage statistics and other information on a scheduled basis.

36. The TIS Gauntlet, Milkyway Blackhole, Checkpoint Firewall-1, DEC AltaVista, Raptor Eagle, and Cyberguard firewalls all supported event notification and alarms. This usually consisted of an email, audio alarm, or page triggered by the occurrence of a pre-defined event (or an event which was not pre-defined, and therefore unexpected), or of the crossing of a defined threshold (such as disk or cpu usage, or number of failed session attempts). These firewalls all provided logging capabilities to record information about the packets flowing through the firewall.

37. The SunScreen firewall monitored and logged packets flowing through the firewall, and also logged session statistics, including the number of bytes and packets transmitted over a TCP, UDP, or IP session. The SunScreen firewall also used SNMP (Simple Network Management Protocol) for event notification. SNMP detected when certain predefined events happened and "alerted" the management station about each event. The SunScreen firewall included a graphical user interface for managing the firewall, which included an SNMP alerts page, a log page, and a traffic statistics page.[27]

38. The Raptor Eagle offered what were probably the most sophisticated alarm features available at the time, encapsulated in what they called their Real-Time Suspicious Activity Monitor (SAM). The SAM allowed an administrator to classify events as one of seven levels, and to assign one of five frequency thresholds (defined in SAM, but not modifiable by the administrator) for triggering alerts. While the Eagle did not include measures such as shutting down sessions as a response option, it did allow alerts to trigger scripts written by the administrator. The Eagle also featured a monitoring program aimed at the security of the firewall host itself; called VultureT, it looked for suspicious processes running on the firewall and shut them down. The Eagle maintained a log describing the opening, closing, and denial of all connections.

---

[27] *See* SunScreen EFS Configuration and Management Guide Release 1.1, Sun Microsystems, Revision A, June 1997; K. Walker and L. Croswhite Cavanaugh, COMPUTER SECURITY POLICIES AND SUNSCREEN FIREWALLS, Sun Microsystems Press 1998.

39. The AltaVista firewall from DEC used a different type of event classification system, based on a series of security states: green, yellow, orange, and red. At each level, the administrator could define the events that would trigger a shift in state and an appropriate response, including shutdown of an individual service or the entire firewall.

40. Both the TIS Firewall Toolkit (in 1993 and later) and the Gauntlet Internet Firewall (circa 1995) logged and reported network events, including denied connections, bytes transferred in network transactions, and number of transactions. The TIS Firewall Toolkit was a freely-available and well-known firewall that was first released in source code form on the Internet in 1993.[28] In addition, a large variety of documentation on the TIS Firewall Toolkit was made publicly available on the Internet well before November 1997, including the following (all docs were made public on the indicated date):

- TIS Firewall Toolkit Configuration and Administration, 2/17/1994,
- TIS Firewall Toolkit Overview, 6/30/1994,
- TIS Firewall User's Overview, 2/8/1994,
- Presentation: Trusted Information Systems Internet Firewall Toolkit – An Overview, 1993, and
- "sample-report" from Firewall Toolkit (11/4/1994).

41. Firewalls used different means to store log data. Some retained data in one or more flat files, either on the firewall host itself, or on a secure logging host on the inside network. Others used databases, in order to make searching and retrieval easier. Log data in 1997 was typically measured in megabytes, not gigabytes as it is today, but nonetheless, manageability of logs and reporting was an important issue and distinguishing factor for firewalls at the time. Firewall-1 provided a graphical log viewer, whereas many other firewalls required use of a text editor.

IV. Disclosures in *Emerald 1997*

[28] *See* F. Avolio, *Firewalls and Internet Security, the Second Hundred (Internet) Years*, Internet Protocol Journal, Cisco Systems, June 1999.

42. I was asked to examine the *Emerald 1997* publication to determine what one of ordinary skill in the art would have understood from this reference at the time of its publication. Specifically, I was asked to focus on what the disclosures relating to a "firewall" would have meant to one of ordinary skill at the time. For the purpose of this analysis, I was asked to assume that one of ordinary skill in the art in 1997 would have been someone with an undergraduate degree in Computer Science with at least three to five years experience in computer programming and network design with an emphasis in network monitoring technology and intrusion detection. Such a person would certainly have been familiar with the concept of a firewall. Firewalls were well-known in the field of computer science generally by 1997, and anyone interested in monitoring a network would have been aware of the importance and usefulness of a firewall in performing network monitoring. One of ordinary skill in the art also would have been familiar with their configuration and operation.[29]

43. *Emerald 1997* disclosed a system called "EMERALD" which implemented a hierarchical system for event monitoring and analysis within an enterprise network:

> *The EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) environment is a distributed scalable tool suite for* ***tracking malicious activity through and across large networks.*** *EMERALD introduces a highly distributed, building-block approach to* ***network surveillance,*** *attack isolation, and* ***automated response.***[30]
>
> The typical target environment of the EMERALD project is a large **enterprise network** with thousands of users connected in a federation of independent administrative *domains.*[31]
>
> EMERALD employs a building-block architectural strategy using independent distributed surveillance monitors that can analyze and respond to malicious activity on local targets, and can interoperate to form an **analysis hierarchy**.[32]

---

[29] *See* F. Avolio, *Firewalls and Internet Security, the Second Hundred (Internet) Years*, Internet Protocol Journal, Cisco Systems, June 1999 (providing a history of firewalls dating back to the late 1980's and noting "[i]n 1997, The Meta Group, and others, predicted that firewalls would be the center of network and internetwork security [Meta Global Networking Strategies File 549, November 24, 1997]").
[30] *Emerald 1997* at 353 (emphasis added).
[31] *Emerald 1997* at 354 (emphasis added).
[32] *Emerald 1997* at 355 (emphasis added).

44. The detection performed by the disclosed EMERALD system was based on analysis of network traffic data which included analysis of network packets:

> Underlying the deployment of an EMERALD monitor is the selection of a target-specific event stream. **The event stream may be derived from** a variety of sources including audit data, **network datagrams,**[33] SNMP **traffic,** application logs, and analysis results from other intrusion-detection instrumentation. … Event records are then forwarded to the monitor's analysis engine(s) for processing.[34]

45. The disclosed EMERALD system deployed multiple network monitors in the enterprise network:

> Service monitors are dynamically deployed within a domain…[35] All EMERALD monitors (service, domain, and enterprise) are implemented using the same monitor code base.[36]

46. The monitors analyzed and responded to suspicious network activity:

> EMERALD employs a building-block architectural strategy using independent distributed surveillance monitors that can **analyze and respond to malicious activity** on local targets, and can interoperate to form an analysis hierarchy.[37]

47. The monitors could analyze a variety of different event streams:

> In general, a monitor may include additional analysis engines that may implement other forms of event analysis… Multiple analysis engines implementing different analysis methods may be employed to **analyze a variety of event streams** that pertain to the same analysis target. These analysis engines

---

[33] A datagram is equivalent to a packet: "datagram n: One packet, or unit, of information, along with relevant delivery information such as the destination address, that is sent through a packet-switching network. See also packet switching." COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997). *Emerald 1997* further discloses analysis of network packets: "EMERALD also extends the statistical-profile model of NIDES, to analyze the operation of network services, network infrastructure, and activity reports from other EMERALD monitors. Various other efforts have considered one of the two types of analysis - signature-based (e.g., Porras [18] has used a state-transition approach; the U.C. Davis and Trident DIDS [4] addresses abstracted analysis for networking, but not scalability; **the Network Security Monitor [7] seeks to analyze packet data** rather than conventional audit trails; Purdue [5] seeks to use adaptive-agent technology) or profile-based. More recent work in UC Davis' GrIDS effort [24] employs activity graphs of network operations to search for traffic patterns that may indicate network-wide coordinated attacks." *Emerald 1997* at 364 (emphasis added).

[34] *Emerald 1997* at 356 (emphasis added).

[35] *Emerald 1997* at 354.

[36] *Emerald 1997* at 356.

[37] *Emerald 1997* at 355 (emphasis added).

> are intended to **develop** significantly lower volumes of abstract ***intrusion* or *suspicion reports***. The profiler and signature engines receive large volumes of event logs specific to the analysis target, and produce smaller volumes of **intrusion or suspicion reports** that are then fed to their associated *resolver*.[38]

48. Hierarchical monitors could receive and correlate the reports of suspicious activity from lower-level monitors:

> Domain-wide analysis forms the second tier of EMERALD's layered network surveillance scheme. A *domain monitor* is responsible for surveillance over all or part of the domain. ***Domain monitors* correlate intrusion reports disseminated by individual service monitors**, providing a domain-wide perspective of malicious activity (or patterns of activity). ... Lastly, **EMERALD enables enterprise-wide analysis**, providing a global abstraction of the cooperative community of domains. **Enterprise-layer monitors correlate activity reports produced across the set of monitored domains.** Enterprise-layer monitors focus on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, and coordinated attacks from multiple domains against a single domain. Through this **correlation and sharing of analysis results**, reports of problems found by one monitor may propagate to other monitors throughout the network.[39]

> "EMERALD monitors incorporate a duplex messaging system that allows them to **correlate activity summaries and countermeasure information in a distributed hierarchical analysis framework.**[40]

A. FIREWALL-SPECIFIC DISCLOSURES

49. *Emerald 1997* disclosed monitoring network packets, network traffic and application logs:

> Underlying the deployment of an EMERALD monitor is the selection of a target-specific event stream. **The event stream may be derived from** a variety of sources including audit data, **network datagrams,** SNMP **traffic, application logs**, and analysis results from other intrusion-detection instrumentation. ... Event records are then forwarded to the monitor's analysis engine(s) for processing.[41]

50. One type of "application log" is a firewall log.

---

[38] *Emerald 1997* at 356 (emphasis added).
[39] *Emerald 1997* at 356 (emphasis added).
[40] *Emerald 1997* at 361 (emphasis added).
[41] *Emerald 1997* at 356 (emphasis added).

51. *Emerald 1997* further disclosed analysis of network services and network infrastructure:

> "EMERALD also extends the statistical-profile model of NIDES, **to analyze the operation of network services, network infrastructure, and activity reports from other EMERALD monitors.**"[42]

52. One type of "network infrastructure" is a firewall. The *Emerald 1997* paper explicitly stated that the EMERALD system monitored network infrastructure such as gateways, routers, and firewalls:

> Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces).[43]
>
> network infrastructure (e.g., routers, filters, DNS, firewalls).[44]

53. The *Emerald 1997* paper also disclosed collecting event records from activity logs:

> At the core of many signature-based expert systems exists an algorithm for accepting the input (in our case activity logs) and, based on a set of inference rules, directing the search for new information.[45]
>
> A set of filtering routines (or log conversion routines with custom filtering semantics) is employed by the analysis engines to gather and format target-specific event records.[46]

54. A firewall log is an activity log. As indicated above, the *Emerald 1997* paper explicitly contemplated converting the information in such firewall activity logs into event records for the network monitors to analyze.

55. *Emerald 1997* further disclosed the use of third-party network management systems (which would include firewalls) to submit information:

> Third-party modules operating as event-collection units may employ EMERALD's external interfaces to submit event data to the analysis engines for

---

[42] *Emerald 1997* at 364 (emphasis added).
[43] *Emerald 1997* at 355. *See also id.* at 358 "For example, the resource object for a domain's router may be reused as other Emerald monitors are deployed for other routers in the domain."
[44] *Emerald 1997* at 354.
[45] *Emerald 1997* at 355.
[46] *Emerald 1997* at 358.

> processing. Such third-party modules would effectively replace the monitor's own event-collection methods.[47]
>
> Of particular interest to the monitoring of network events is our planned incorporation of a commercially available network management system as a third-party module. That system will deliver monitoring results relating to security, availability, performance, and other attributes.[48]

56. Thus, the *Emerald 1997* paper explicitly disclosed that monitors would perform analysis based on network infrastructure such as a firewall, and the logs produced from a firewall.

B. DISCLOSURE OF NETWORK TRAFFIC DATA CATEGORIES

1. Claimed categories of network traffic data

57. I was asked to review the patents-in-suit to gain an understanding of the categories of network traffic data or measures of network packets that the claims require be monitored. I reviewed the patents in detail, including the claims, in order to gain an understanding of these terms. My review of the claims indicated the following different types of claimed network traffic:

- data transfers, errors, network connections ('338 claim 1)
- network packet data transfer commands ('338 claim 2, '203 and '615 claim 1)
- network packet data transfer errors ('338 claim 3, '203 and '615 claim 1)
- network packet data transfer volume ('338 claim 4) and network packet data volume ('203 and '615 claim 1)
- network connection requests ('338 claim 5, '203 and '615 claim 1)
- network connection denials ('338 claim 6, '203 and '615 claim 1)
- correlation of network connection requests and network connection denials ('338 claim 7)
- error codes included in a network packet ('338 claim 8, '203 and '615 claim 1)

[47] *Emerald 1997* at 357.
[48] *Emerald 1997* at 363.

- privilege error code ('338 claim 9)
- error code indicating a reason a packet was rejected ('338 claim 10)
- network connection acknowledgements ('615 claim 1)
- network packets indicative of well-known service protocols ('615 claim 1)

58. I understand that currently neither party has proposed a claim construction defining these terms. Thus, I have been asked to use the ordinary meaning of each term. I understand that claim language is generally construed in accordance with its ordinary and customary meaning to those skilled in the relevant art as of the date of the invention. I also understand that claim terms should be given the meaning that is objectively discerned from the specification and/or the patent's prosecution history by one of ordinary skill in the art as of the date of the invention, even if that meaning differs from the term's ordinary and customary meaning.

2. Legal standard

59. I have been informed that the doctrine of inherent anticipation applies when the evidence makes it clear that "the missing descriptive matter is necessarily present in the thing described in the reference, and it would be so recognized by persons of ordinary skill." In my opinion, although the *Emerald 1997* reference does not recite verbatim the claimed network traffic data categories, several of these categories are necessarily present in the disclosure and would have been recognized as present by one of ordinary skill in the art.

60. Firewalls in 1997 performed a set of common functions in monitoring, filtering, and logging packets, which would have been known to one of ordinary skill in the art at the

time. In configuring a firewall to conform to the requirements of the disclosed EMERALD monitoring system, as of the time of the *Emerald 1997* disclosure, one would have necessarily analyzed multiple different claimed categories of network traffic data or measures of network packets, including: network connections (including both network connection requests and network connection denials), and data transfers (including network packet data volume).

3. Network connections

61. Two of the claimed "network traffic data" categories are "network connection requests" and "network connection denials." The claims also include "network connections" as a "measure of the network packets." The ordinary meaning of a "network connection" is a communication link between two communication computers or devices.[51] A review of the patents' common specification reveals that the inventors did not use this term in a manner different than its ordinary meaning. For example, Fig. 6 illustrates a "network connection 52" that links a "digital computer 56" to any other entity on the network.[53] Thus, the ordinary meaning of a "network connection request" is any network traffic data indicating a request for a network connection. The ordinary meaning of a "network connection denial" is any network traffic data indicating a denial of a network connection.[54]

62. First, the *Emerald 1997* reference disclosed monitoring network connectivity, which one of skill in the art would understand to encompass monitoring network connections, as well as network connection requests and denials:

> This layered analysis hierarchy provides a framework for the recognition of more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an entire network enterprise.[55]

---

[51] "network n. A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephones or other communications links." COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997).
[53] '338 Fig. 6, col. 14:42-49.
[54] The patent specification also states that "network connection information" can include analysis of the packets forming the TCP three-way handshake (SYN ACK and RST). *See* '338 col. 13:31-49.
[55] *Emerald 1997* at 355.

63. In addition to generally disclosing the monitoring of network connections, *Emerald 1997*, like the patents themselves, disclosed that logs from entities such as firewalls may be used to gather event data for analysis. Firewalls in 1997 monitored and logged network connections, including network connection requests and denials, and thus analysis of these three categories of network traffic data is inherent in the *Emerald 1997* disclosure.

64. The patents' specification provides several examples of information (event streams) corresponding to network connection requests / denials:

> "Selection of packets can be based on different criteria. Streams of event records can be derived from discarded traffic (i.e., packets not allowed through the gateway because they violate filtering rules)..."[56]

Discarded traffic indicates a network connection denial.

> "pass-through traffic (i.e., packets allowed into the internal network from external sources)..."[57]

Pass-through traffic indicates a network connection request.

65. Furthermore, the specification discloses that such information can be gathered from the logs of network entities such as routers, gateways, and firewalls[58]:

> Event records can also be produced from other sources of network packet information such as report logs produced by network entities.[59]

66. As shown previously, *Emerald 1997* disclosed that the EMERALD system monitored network traffic and network packets. The *Emerald 1997* paper further disclosed that the EMERALD system monitored network infrastructure such as firewalls. The *Emerald 1997* paper also disclosed collecting event records from logs.

67. When configuring a firewall, one must define what kinds of data pass through and what kinds of data are blocked.[60] This setup defines both permitted host computers, and

---

[56] '338 col. 5:4-7.
[57] '338 col. 5:7-8.
[58] '338 col. 3:43-44.
[59] '338 col. 5:4-25 (network entities include gateways, routers, firewalls).
[60] "To set up your firewall, you must therefore define what kinds of data pass and what kinds

permitted protocols or services.[61] Thus, firewall configuration requires one to set the firewall to monitor: (1) network connection requests for packets that will be allowed to pass through the firewall ("pass-through traffic"); and (2) network connection denials for packets that violate the rules set up for entry ("discarded traffic"). In so doing, one necessarily monitors "network traffic data" corresponding to the "network connection requests and denials" categories.

68. In addition to monitoring such network connections, firewalls in 1997 routinely logged for review packets allowed in, and packets blocked or discarded.[62] Such network connections requests and denials would have been present in the firewall's activity logs, which the system disclosed in *Emerald 1997* used as a source of event data.

69. For example, SunScreen firewall user manuals from 1997 clearly indicate that this firewall logged information about network connections, including network connection requests and denials. The SunScreen EFS Configuration and Management Guide Release 1.1, Sun Microsystems, Revision A, June 1997 states that one of the SunScreen EFS features was

---

are blocked. ... Default permit With this strategy, you give the firewall the set of conditions that will result in data being blocked. Any host or protocol that is not covered by your policy will be passed by default. Default deny With this strategy, you describe the specific protocols that should be allowed to cross through the firewall, and the specific hosts that may pass data and be contacted. The rest are denied." S. Garfinkel and G. Spafford, PRACTICAL UNIX & INTERNET SECURITY at 638 (O'Reilly 1996) (emphasis added).

[61] "Firewalls can be used to block access to particular sites on the Internet, or to prevent certain users or machines from accessing certain servers or services." S. Garfinkel and G. Spafford, PRACTICAL UNIX & INTERNET SECURITY at 639 (O'Reilly 1996).

[62] *See* D. B. Chapman and E. Zwicky, BUILDING INTERNET FIREWALLS, at 179-80: "Make sure the packet filtering router gives you the option of logging all of the packets it drops. You want to know about any packets that are blocked by your packet filtering rules. These rules reflect your security policy and you want to know when somebody attempts to violate that policy. The simplest way to learn about these attempted violations is through such a log. You'd also like to be able to log selected packets that were accepted. For example, you might want to log the start of each TCP connection." *See also id.* at 400: "In particular, you want to log the following cases:

- All dropped packets, denied connections, and rejected attempts
- At least the time, protocol, and user name for every successful connection to or through your bastion host
- All error messages from your routers, your bastion host, and any proxying programs."

"[l]ogging session statistics, including the number of bytes and packets transmitted over a TCP, UDP, or IP session."[63] As explained previously, a "session" is synonymous with a connection. The manual also explains that "packets matching Fail rules or packets that are dropped because they do not match any rule are logged"[64] indicating that the firewall logged discarded traffic.

70. The SunScreen firewall used sas_logdump to output data into log files about sessions. The manual explains that "[s]essions can be either TCP sessions (connections), UDP sessions (request/response pairs), or IP sessions (traffic of a particular IP type between a pair of hosts)."[65] The log entry format also included a variable <finalstate> (a binary value representing the final state of TCP connections).[66] A value of <1> indicated a connection was not established because no response to a SYN packet was received. A value of <2> indicated a connection was not established because no response to a SYN/ACK packet was received.[67] A value of <4> indicated a successfully closed connection. Clearly, the SunScreen firewall in 1997 monitored and logged information about network connections, including successful and failed connections indicating connection requests and denials.

71. Thus, analysis of two of the "network connection requests/denials" embodiments from the patents-in-suit are the natural result flowing from the operation as taught by the EMERALD system disclosed in *Emerald 1997*. Furthermore, this disclosure would have been recognized by one of ordinary skill at the time.

4. Data transfers / network packet data volume

---

[63] SunScreen EFS Configuration and Management Guide Release 1.1, Sun Microsystems, Revision A, June 1997 at page xxv [SUN_0000501-SUN_0000856].
[64] *Id.* at page 6-1.
[65] *Id.* at page 6-2.
[66] *Id.* at page 6-4.
[67] The manual also noted that "[a] large number of these sessions could indicate a SYN attack." *Id.* at page 6-4.
[69] '338 col. 5:31-36 (emphasis added).

72. An additional claimed category of network traffic data is "network packet data volume" or "network packet data transfer volume" (I do not believe there is a distinction between the meaning of these two phrases). Furthermore, a measurement of "network packet data volume" would be a measurement of "data transfer" as well. The plain meaning of "network packet data volume" is any information illustrating the size of a particular set of network traffic in a given time interval. The patents' specification provides several examples of event streams that correspond to the "network packet data volume" category, including the number of packets, number of kilobytes, and number of fingers or failed login requests:

> A monitor 16 can also construct interval summary event records, which contain accumulated network traffic statistics (e.g., **number of packets and number of kilobytes transferred**). These event records are constructed at the end of each interval (e.g., once per N seconds). Event records are forwarded to the analysis engines 22, 24 for analysis.[69]
>
> For example, monitors can encode thresholds to monitor activity such as the **number of fingers, pings, or failed login requests** to accounts such as guest, demo, visitor, anonymous FTP, or employees who have departed the company.[70]

73. A standard firewall in 1997 monitored the amount of packet data sent over each connection.[71] Such monitoring corresponds to the "network packet data volume" category of "network traffic data." It was also standard practice for firewalls to log the number of packets and kilobytes of data transferred over each particular connection.[72]

---

[70] '338 col. 7:50-55 (emphasis added).

[71] "A firewall can be used to monitor communications between your internal network and an external network. For example, you could use the firewall to log the endpoints and amount of data sent over every TCP/IP connection between your organization and the outside world." S. Garfinkel and G. Spafford, PRACTICAL UNIX & INTERNET SECURITY at 639.

[72] *See* M. Ranum and F. Avolio, "A Toolkit and Methods for Internet Firewalls," June 1994 (http://www.avolio.com/papers/fwtk.html). This paper, presented at the USENIX Summer 1994 Technical Conference, June 6 - 10, 1994, in Boston (http://www.usenix.org/publications/library/proceedings/bos94/index.html) states: "All traffic can be logged and summarized." In the TIS Firewall Toolkit (FWTK) documentation (doc directory in the source kit (http://www.fwtk.org/fwtk/download/downloading.html), Presentation: Trusted Information Systems Internet Firewall Toolkit – An Overview, 1993 states: "Connection logs maintained" (p. 30); "All connections and amount of data transferred are logged" (p. 32); and "All connections and traffic logged" (p. 33). *See also* TIS Firewall Toolkit Overview, 6/30/1994 and "sample-report" from Firewall Toolkit (11/4/1994).

74. For example, the SunScreen firewall manuals clearly demonstrate that the firewall monitored and logged multiple different types of statistics on "network packet data volume." Session records from SunScreen included <fwdpackets> (the number of packets from the source to the destination address), and <fwdbytes> (the number of bytes sent from the source to the destination address). Packets and bytes sent from the destination address to the source address were similarly logged.[73]

75. Thus, one of ordinary skill in the art would have recognized monitoring and logging "network packet data volume" as an inherent feature of setting up an EMERALD-type system.

76. In addition, *Emerald 1997* also disclosed monitoring "finger" and "login" requests, as well as the ability to detect "floods" of information such as a denial-of-service attack:

> Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces).[74]
>
> Network services include features common to many network operating systems such as mail, HTTP, FTP, **remote login**, network file systems, **finger**, Kerberos, and SNMP.[75]
>
> EMERALD has significant advantages over more centralized approaches... It can detect not only local attacks, but also coordinated attacks such as **distributed denials of service**.[76]

77. A "finger" request is a standard protocol commonly used to look up information about users logged onto a system.[77] Monitoring for frequent or repeated "finger" requests was well-known in 1997, because the "finger" command was a known precursor to an attack.[78]

---

[73] SunScreen EFS Configuration and Management Guide Release 1.1, Sun Microsystems, Revision A, June 1997 at pages 6-3 to 6-4.
[74] *Emerald 1997* at 355.
[75] *Emerald 1997* at 354 (emphasis added).
[76] *Emerald 1997* at 365 (emphasis added).
[77] *See* W. Cheswick and S. Bellovin, FIREWALLS AND INTERNET SECURITY, at 33.
[78] *See* W. Cheswick and S. Bellovin, FIREWALLS AND INTERNET SECURITY, at 133 ("Generic finger attempts are often used to gather login names, personal information, and account usage

Similarly, the need to monitor for frequent or repeated failed "login" requests was well-known in 1997, because this behavior also was a common precursor to an attack.[79] In addition, a common form of a network "denial of service" attack is a flood of messages such as requests for login.[80]

78. Thus, the specific teaching to monitor "finger" and "login" requests as well as detect "denial of service" attacks, combined with the common knowledge that a grouping of such requests signaled potential danger, illustrates that *Emerald 1997* inherently disclosed monitoring "network packet data volume" as measured by a quantity of finger and/or login requests.

5. Firewall logs provide "network traffic data"

79. Three of the patents-in-suit require that the detection of suspicious network activity be "based on analysis of network traffic data" (see, e.g., '203 claim 1, '212 claim 1, '615 claim 1). One of the patents-in-suit requires "network packets handled by a network entity" (see '338 claim 1). Analysis of information from a firewall log constitutes analysis of network traffic data. It also constitutes a measure of "network packets handled by a network entity." A firewall log provides information about the network traffic or packets that are or were flowing through the firewall. A firewall log would provide, for example, a measure of the amount of "network packet data volume" flowing through the firewall as an input to a monitor performing analysis in order to allow the monitor to detect suspicious network activity.

---

information for hacking attempts."), at 184-86 (Fig. 11.3, showing logged volume of the "distribution of evil finger requests").

[79] *See* D. B. Chapman and E. Zwicky, BUILDING INTERNET FIREWALLS, at 403 (explaining the dangers of repeated attempts to login, and stating "[t]here or more attempts to log in at 2 a.m., and someone is trying to break in."), at 400 ("For example, although you should log failed login attempts, you should not log the password that was used..."); *see also* W. Cheswick and S. Bellovin, FIREWALLS AND INTERNET SECURITY, at 185 (Fig. 11.2, showing logged volume of logins and hostile login attempts).

[80] *See* S. Garfinkel and G. Spafford, PRACTICAL UNIX AND INTERNET SECURITY, at 775-76.

80. In fact, the *Emerald 1997* publication expressly indicates that this is exactly what is contemplated. As explained in the reference, the detection performed by the EMERALD monitor is based upon an event stream, which may be derived from a variety of sources including "application logs":

> Underlying the deployment of an EMERALD monitor is the selection of a target-specific event stream. **The event stream may be derived from** a variety of sources including audit data, **network datagrams,** SNMP **traffic, application logs**, and analysis results from other intrusion-detection instrumentation. ... Event records are then forwarded to the monitor's analysis engine(s) for processing.[81]

The *Emerald 1997* reference expressly disclosed monitoring an event stream from a firewall or firewall log, and thus inherently disclosed monitoring the particular different categories of network traffic data that were monitored by firewalls at the time: network connections, including network connection requests and network connection denials, and data transfers, including network packet data volume and network packet data transfer volume.

V. The *Emerald 1997* paper disclosed monitor deployment at both a "firewall" and a "proxy server."

81. The '615 patent's independent claim 84 contains the limitation "wherein at least one of the network monitors is deployed at ... proxy servers"[82] and independent claim 64 contains the limitation "wherein at least one of the network monitors is deployed at a firewall."[83] The patents' specification does not explicitly define either the term "firewall" or "proxy server."[84] Based upon the plain meaning of these terms, both of these limitations are anticipated by the *Emerald 1997* disclosure.

---

[81] *Emerald 1997* at 356.
[82] '615 col. 20:56-59.
[83] '615 col. 19:32-33.
[84] The patents' specification does state that both firewalls and proxy servers are "network entities." '338 col. 3:44-45. P. Porras and A. Valdes, *Live Traffic Analysis of TCP/IP Gateways*, Nov. 10, 1997 states that both firewalls and proxy servers produce "report logs." *Id.* at p. 5.

82. As explained previously, *Emerald 1997* disclosed deploying monitors at infrastructure such as a firewall. A proxy server is effectively synonymous with a firewall, as shown by the dictionary definitions of both terms:

> **firewall** *n.* A security system intended to protect an organization's network against external threats, such as hackers, coming from another network, such as the Internet. A firewall prevents computers in the organization's network from communicating directly with computers external to the network and vice versa. Instead, all communication is routed through a proxy server outside of the organization's network, and the proxy server decides whether it is safe to let a particular message or file pass through to the organization's network.
>
> **proxy server** *n.* A firewall component that manages Internet traffic to and from a local area network (LAN) and can provide other features, such as document caching and access control. ... *See also* firewall.[85]

83. One of ordinary skill in the art in 1997 would have understood that a firewall includes a proxy server, and that disclosure of deploying a monitor at a firewall necessarily also encompassed deployment at a proxy server.

84. I declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both (18 U.S.C. 1001).

Signed: June 9, 2006

Frederick M Avolio

[85] COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997).

Frederick Michael Avolio

Career Overview

Fred Avolio is the president and founder of Avolio Consulting, Inc., a Maryland-based corporation specializing in computer and network security, and dedicated to improving the state of corporate and Internet security through education and testing. Avolio is a recognized computer and network security expert, and has been active in the UNIX, TCP/IP communities since 1979. Since 1992, he has specialized in Internet and computer security. Avolio Consulting, Inc. started in mid-1998. Since that time he has worked for small security start-ups, vendors with security products such as WatchGuard , and security-related companies, including TruSecure . He splits his time between training, consulting, and writing.

In the position of Vice President at Trusted Information Systems, Inc., Avolio was involved in technology and company analysis for merger and acquisition activity, and helped set security product direction. He was also Corporate Information Security Officer. Previously, at TIS, he worked in TIS' network security consulting group and was product manager and development manager for TIS' Gauntlet Internet Firewall, and its predecessor, the TIS Internet Firewall Toolkit. The latter was part of a DARPA sponsored contract for the White House.

Before joining TIS, Avolio was a senior consultant and senior manager with Digital Equipment Corporation. Among other duties there, he managed and maintained one of DEC's Internet gateways and help productize the DEC SEAL firewall. Earlier he worked at NSA, supporting UNIX systems, specializing in electronic mail.

Avolio is a highly-rated speaker and contributor to international conferences including CSI, Networld+Interop, MIS, and USENIX. He has lectured and provided consulting services on Internet gateways and firewalls, Internet security, security policy development, electronic mail configuration, and other related topics for both government and industry.

Publications and Papers

Avolio posts entries to his weblog on various subjects, including network and computer security. Please see his "blog" at URL http://www.avolio.com/weblog/. He also writes whitepapers, product reviews, and magazine columns. Please see the list at URL http://www.avolio.com/papers.html.

Employment History

June 1998 – Present, principal and founder of Avolio Consulting, Inc.

November 1992 – May 1998, Trusted Information Systems. Vice President of Technology Marketing. Responsibilities included M&A activity, product positioning in the market, relations with press and industry analysts. He was also Corporate Information Security Officer. Before that, Avolio was Vice President of Marketing for the Network Security Products group in TIS. Before that, he was product manager and development manager for the Gauntlet and the Firewall Toolkit products and worked in commercial security consulting. He started at TIS as a principal project leader.

April 1984 – November 1992, Digital Equipment Corporation. Avolio was a senior consultant and senior manager with Digital Equipment Corporation, leading a group of top level sales support specialists for the Mid Atlantic Area of Digital. Previously, he was a senior consultant for UNIX

and TCP/IP networking. Among other duties there, he managed and maintained one of DEC's Internet gateways and was instrumental in producing Digital's Internet firewall product.

January 1979 – April 1984, National Security Agency. Avolio was responsible for UNIX system specification and deployment in support of field organizations. He also managed and programmed UNIX systems.

Education

Master of Science, Computer Science, Indiana University, 1979.

Bachelor of Science, Computer Science, University of Dayton, April 1977.

Contact Information

16228 Frederick Road
PO Box 609
Lisbon, MD 21765–0609

fred@avolio.com
www.avolio.com

410–489–5215 (home)
443–283–8028 (office)
443–414–5215 (mobile)

Publications and Papers: *http://www.avolio.com/papers.html*

Columns, Regular and Irregular

Fred Avolio regularly posts on security and other topics. He was a member of WatchGuard Technologies, Inc.'s LiveSecurity Advisory Council, and for a few years wrote a column for their LiveSecurity Service, a service that allows their subscribers to stay current on security issues. We republish them with WatchGuard's permission.

He wrote the "Just the Basics" column for *Information Security Magazine* as well as writing for searchSecurity.com. He sometimes contributes to LURHQ Corporation's *On the Radar* newsletter.

Articles, Presentations, & Papers

Producing Your Network Security Policy. This paper, written for WatchGuard Technologies, Inc., lays out a common-sense approach to writing corporate security policies that makes them easier to draft, maintain, and enforce. Our "question and answer" approach requires no outside consultants. [What was I thinking!?] Instead, you can use your in-house knowledge and resources to yield a brief, usable, and – most importantly – understandable policy document, in a reasonable amount of time. To help you generate such a policy, this paper clears away some misconceptions about the purpose of network security; details the process of writing the policy; then explains how to keep refining the drafted policy.

Painless PGP. PGP Corp. delivers practical PKI deployment for securing e-mail with PGP Universal. This is a "Test Center" product evaluation from the December 2003 Information Security Magazine.

A short history of firewalls

Security Review: SSL VPNs. A whitepaper I wrote for Aventail.

"Sidewinder Runs the Gauntlet," From the April 2003 *Information Security Magazine*, a review of the Sidewinder G2 Firewall Appliance.

"Gateway Guardians," From the January 2003 *Information Security Magazine*, a review of 5 E-mail firewalls.

The Secure Email collection. A collection of my papers and articles on the subject.

I reviewed an e-mail security product called IronMail (from CipherTrust) for *Information Security Magazine*. It's in the print edition and on-line at http://www.infosecuritymag.com/articles/october01/departments_products2.shtml.

Signed, Sealed, and Delivered. A cadre of new e-mail security applications aims to solve the problems that have long plagued PGP and S/MIME. Written with Dave Piscitello.

The Rise and Fall of Internet Security. I delivered this paper at the Spring 2000 Internet Security Conference, in San Jose. I discuss the state of Internet security. It isn't good. (Well, the paper is good... you know what I mean.)

"Best Practices in Network Security,". Network security policies can touch on every aspect of every employee's interaction with the network. This Network Computing Magazine March 20, 2000 article will provide you with a solid security framework, built on the right premises.

In October 1999, as a guest columnist for David Strom's Web Informant email newsletter, I wrote about Email paranoia, coming out in favor of it.

"e-Business and the Need for 'Air Gap' Technology" is a (PDF format) white paper describing Whale Communications' e-Gap™ product, a commmunications "air gap" for e-business.

Buyer's Guide: Biometrically Speaking is an article I wrote for Network Computing Magazine dated August 23, 1999. It gives an overview of biometric technology.

In July 1999, I was a guest columnist for David Strom's Web Informant e-mail newsletter. It was reprinted in Byte Magazine. I was asked to try to break into his new site.

The Castle Defense A primer for enterprise system and network protection. A Performance Computing Special Report from the July 1999 issue.

Firewalls and Internet Security, the Second Hundred (Internet) Years An overview of the evolution of Internet firewalls with a look towards the future. Published in the June 1999 issue of Cisco's *The Internet Protocol Journal*.

Firewalls: Are We Asking Too Much? Information Security magazine cover story, May, 1999. Allowing a new service through a firewall is easy. Doing it while maintaining the same high level of security isn't.

Security Axioms. Some are true, some just sound true. It is important to know which is which.

Software Review: Sendmail Pro. This is a Performance Computing April 1999 review of Sendmail, Inc.'s first commercial Sendmail product. (I liked it.)

Intrusion Detection Joins Net Security Arsenal, Internet World, March 22, 1999. An overview of the passive and active techniques that work together to help systems administrators stay on top of intrusion perils.

MailGuardian delivers transparent security to users. This is an InforWorld February 8, 1999 review of Vanguard Security Technologies' MailGuardian product. MailGuardian provides e-mail security.

The Foundations of Enterprise Network Security, Originally published in *Data Security Management*, February 1999. Copyright © 1999 Auerbach Publications. User by permission. This article discusses the initial work that must be done to establish a network and computer security perimeter. Specifically, we discuss business needs analysis, risk assessments, security policy development, and the selection of mechanisms and establishment of methods.

Identity Confirmed, An "Issues and Trends" piece published in Network World, August 24, 1998. This is a discussion of biometric authentication devices, such as fingerprint readers, voice recognition systems, and retinal scanners.

Some Important VPN Questions Answered (A CSI Interview with Fred Avolio), from the Computer Security Alert Number 185, August 1998.

A Multi-Dimensional Approach to Internet Security, from Volume 2.2 of the ACM netWorker magazine, 1998. This article discusses all the things that make up the establishment of computer and network security. Firewalls are not enough.

A Computer and Network Security Primer, 1998. A short paper written to explain some of the basic terminology.

Application Gateways and Stateful Inspection, revised January 1998. There has been much

discussion and marketing hype surrounding application gateways and stateful multilevel inspection as architectures for firewall development. After a lengthy discussion on the firewalls mailing list, the authors wrote and distributed this paper. It is the result of experience, observation, and input from the members of the firewalls mailing list.

An Approach to Computer Security, originally published in the TIS Data Security Letter in 1996. This is a short editorial arguing for doing the groundwork of network security.

Firewalls and Virtual Private Networks, 1996. A brief article discussing VPNs and how they are supported by Internet firewalls.

Tracing Electronic Mail, 1996 Based on a short training session for the US Secret Service on the methods to use to trace electronic mail, this paper should be helpful for system managers and postmasters.

Security on the Internet -- A Viewpoint . This editorial appeared in the Proceedings of the 17th National Computer Security Conference, October 1994. Basic point: firewalls are not enough.

The Seven Tenets of Good Security. Rules to live by.

A brief history of the TIS Internet Firewall Toolkit (FWTK), copied over from the "unofficial" user site.

Network Security: Building Internet Firewalls, Originally published in the BUSINESS COMMUNICATIONS REVIEW, January 1994. This magazine articles is an introduction to Internet Firewalls and, though old by Internet standards, is still useful.

A Toolkit and Methods for Building Internet Firewalls, proceedings of the summer USENIX conference, June 1994. In this paper, Marcus Ranum and Fred Avolio discuss one of the results of the DARPA project to establish and secure WhiteHouse.Gov and the President's e-mail. Specifically, it is the first formal description of the TIS Internet Firewall Toolkit (FWTK).

A Network Perimeter with Secure External Access, proceedings of the ISOC NDSS Symposium, February 1994. This paper, coauthored by Marcus Ranum, discusses a research project for DARPA in which two of the goals were to raise the level of network and computer security for the White House and to securely put the President on-line for e-mail access.

Books

With Paul Vixie, Sendmail Theory and Practice, Second Edition , published by Butterworth-Heinemann, December 2001. This book explains how and why Sendmail does what it does and provides "cookbook recipes" and simplified explanations on how to manage a mail system. The authors progress from the simple to the complex, providing knowledge essential for both the interested user and the experienced system manager. Updated for Sendmail version 8.11.

Book Reviews

KNOW IT Security: Secure IT Systems Casino Style by Jim Litchko. "In this book Jim explains all of the key aspects -- the Essentials -- of IT security for the manager."

The Myth of Homeland Security by Marcus J. Ranum. Ranum's book is engaging, unsettling, entertaining, and disturbing. Yet, I think it is an accurate assessment of the morass that is "homeland security." Fred Avolio reviewed this on Amazon.com.

Removing the Spam: Email Processing and Filtering by Geoff Mulligan. Small but thorough book covering email configuration with an eye towards stopping spam. This review appeared in Cisco's The Internet Protocol Journal, March, 2000.

Information Warfare and Security , by Dorothy Denning. Denning's book about all aspects of information warefare is incredibly informative as well as being an enjoyable read. Fred Avolio reviewed this for Cisco's The Internet Protocol Journal, September, 1999.

Internet Cryptography , by Richard Smith. This is an excellent book covering cryptography and how it is used in security solutions on the Internet. Written by an expert, reviewed by Fred Avolio. Originally published in Cisco's The Internet Protocol Journal, March, 1999.

Exhibit B

1. U.S. Pat. Nos. 6,321,338, 6,484,203, 6,708,212, 6,711,615 and associated file histories [SYM_P_0071535-0071549], [SYM_P_0071550-0071563], [SYM_P_0071564-0071579], [SYM_P_0071580-0071598].
2. Joint Claim Construction Statement, Filed March 17, 2006
3. P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20th National Information Systems Security Conference, October 7, 1997 [SYM_P_0554932-0554966].
4. P. Porras and A. Valdes, *Live Traffic Analysis of TCP/IP Gateways*, Nov. 10, 1997 [SYM_P_0068844-0068865].
5. ICSA 2nd Annual Firewall Buyer's Guide 1996 [SYM_P_0548919-0548989].
6. ICSA 3rd Annual Firewall Buyer's Guide 1998 [SYM_P_0548792-0548884].
7. B. Chapman & E. Zwicky, BUILDING INTERNET FIREWALLS, O'Reilly and Associates, 1995 [SYM_P_0498347-0498742].
8. *Web Security Sourcebook*, Rubin, Geer & Ranum, John Wiley & Sons, 1997 [SYM_P_0600860-0600865].
9. *Intranet and Internet Firewall Strategies*, E. Amoroso & R. Sharp, ZD Press, 1996 [SYM_P_0600847-0600859].
10. "Buyer's Guide: Keeping the Huns at Bay," Joel Snyder, *Network World Magazine*, 2/3/97 [SYM_P_0549937-0549944].
11. "Fortifying Your Firewall," Pete Morrissey, *Network Computing Magazine*, 2/7/97 [SYM_P_0535498-0535512].
12. R. Bace, INTRUSION DETECTION (Macmillan Technical Publishing 2000) [SYM_P_0082132-0082148].
13. S. Garfinkel and G. Spafford, PRACTICAL UNIX & INTERNET SECURITY at 289-92 (O'Reilly and Assoc. 2nd ed. 1996) [SYM_P_0498070-0498346].
14. COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997) [SYM_P_0601002-0601012].
15. D. Comer and D. Stevens, INTERNETWORKING WITH TCP/IP, VOL. III, Chap. 18 "Application Level Gateways," (Prentice-Hall 1993) [SYM_P_0600882-0600915].
16. L.T. Heberlein et al., *A Method to Detect Intrusive Activity in a Networked Environment*. Proceedings of the Fourteenth National Computer Security Conference, at 362-71, Washington, D.C., 1-4 Oct. 1991, NIST/NCSC [SYM_P_0069355-0069365].
17. S. McCanne and V. Jacobson, *The BSD Packet Filter: A New Architecture for User-level Packet Capture*, Dec. 19, 1992 [SYM_P_0070068-0070078].

18. W. Cheswick and S. Bellovin, FIREWALLS AND INTERNET SECURITY – REPELLING THE WILY HACKER (Addison-Wesley Pub. Co. 1994) [SYM_P_0498743-0498951].

19. http://csrc.nist.gov/publications/nistbul/itl97-03.txt [SYM_P_0600876-0600881]

20. F. Avolio, *Firewalls and Internet Security, the Second Hundred (Internet) Years*, Internet Protocol Journal, Cisco Systems, June 1999 [SYM_P_0600866-0600875].

21. M. Ranum and F. Avolio, "A Toolkit and Methods for Internet Firewalls," June 1994 (http://www.avolio.com/papers/fwtk.html) [SYM_P_0603060-0603068].

22. SunScreen EFS Configuration and Management Guide Release 1.0, Sun Microsystems, Revision A October 1996 [SUN_0002005-0002174].

23. SunScreen SPF-100 SPF-100G Administrator's Handbook, Sun Microsystems, Revision A April 1996 [SUN_0002175-0002478].

24. SunScreen EFS Configuration and Management Guide Release 1.1, Sun Microsystems, Revision A June 1997 [SUN_0000501-0000856].

25. K. Walker and L. Croswhite Cavanaugh, COMPUTER SECURITY POLICIES AND SUNSCREEN FIREWALLS, Sun Microsystems Press 1998 [SYM_P_0602762-0602909].

26. Firewall Toolkit source code [SYM_P_0502521-0503248].

27. TIS Firewall Toolkit Configuration and Administration, 2/17/1994 [SYM_P_0602955-0602968].

28. TIS Firewall Toolkit Overview, 6/30/1994 [SYM_P_0602978-0602991].

29. TIS Firewall User's Overview, 2/8/1994 [SYM_P_0603055-0603059].

30. Presentation: Trusted Information Systems Internet Firewall Toolkit – An Overview, 1993 [SYM_P_00602992-0603048].

31. "sample-report" from Firewall Toolkit (11/4/1994) [SYM_P_0603049-0603054].

In addition, I spoke with Mr. Todd Heberlein regarding the contents of this report.